



COMP232

Identification and authentication

CNS, Section 2.4
WSPC, Chapter 6

Identification, authentication, authorisation

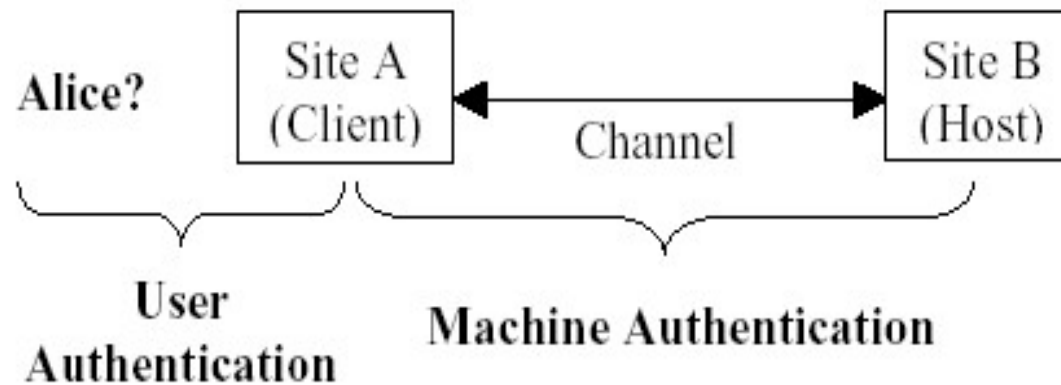
- Three closely related concepts:
- **Identification:** associating an identity with a subject (“Who are you?”)
- **Authentication:** establishing the validity of something, such as an identity (“Are you indeed the entity you claim you are?”)
- **Authorisation:** associating rights or capabilities with a subject (“What rights (authority) do you have?”)

Authentication

- **Authentication** is the process of verifying the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in the system
- Authentication is used for the purpose of performing **trusted communications** between parties for computing and telecommunications applications.

Authentication

- **Machine-by-machine** authentication
- **Human-by-machine** authentication (user authentication)



(Picture by Lawrence O’Gorman, Proc. of IEEE , Dec 2003)

User vs Machine authentication

- User authentication is much less secure than machine authentication
- Example:
 - encryption algorithm in AES standard uses the keys up to 256 bits long;
 - a 256-bit key is too long for most humans to remember, so in practice this key is stored in a computer file protected by a more memorable password;
 - Here is the problem: human tend to choose an easily guessable password
- In many cases humans are “weakest links” of otherwise secure systems

Authentication techniques

- Authentication techniques can be based on
 - Passwords (knowledge-based, “what you know”)
 - Tokens (object-based, “what you have”)
 - Biometrics (ID-based, “who you are”)

Password-based techniques

- **Password:** a word, a phrase, or personal identification number that is kept as a secret and is used for authentication;
- Very popular and for many purposes adequate techniques, which don't need a special hardware;
- The main problem:
 - short memorable password can be guessed or searched by attacker;
 - Long and random password is difficult to remember

Other problems with passwords

- Before one can use a computer system, or a service, one needs a password
 - Password may be intercepted on its way to the system
 - Password may be forgotten
 - Password may be passed to other people
-
- Although these problems can be dealt with, there is no absolute solution

“New” type of attacks – acoustical spying

- Researches at UC Berkley have demonstrated how one can recover up 96 percent of text using using an audio recording of the sounds generated by typing on a computer keyboard (September, 2005)
- Each keystroke makes a relatively distinct sound when hit. Using statistical learning theory, the program can categorize the sounds of each key and produce a good first guess, which then improved by using spelling and grammar checks
- Having a small microphone nearby a computer allows one to find out what password (for example) has been used.

Token-based authentication

- **Physical token** (identity token, security token) is physical device which perform or help authentication, such as:
 - Door key
 - Magnetic, or radio-frequency based access cards
 - Bankcard
 - Smartcard
 - Etc
- Authentication is based on what you have

Types of tokens

- This can be a secure storage device containing
- passwords, such as a bankcard, remote garage door opener, or smart card.
- This can also be an active device that yields *one-time passcodes* (*machine generated passwords*), either
 - *time-synchronous*
 - *or challenge-response*

Problems with tokens

- The token doesn't really "prove" who an owner of the token is – anybody who has possession of the token can gain access
- If the token is lost, the owner can not have an access, despite his/her identity has not changed
- Some tokens may be easily copied or forged

Multi-factor authentication techniques

- To increase security In some applications tokens are combined with other means of identification, such a passwords (PINs).
- **Examples:**
 - banking cards as tokens, and PINs as passwords
 - Mobile phone two-factor authentication:
 - password +
 - one time passcode sent by SMS/or Voice (proof of ownership of mobile phone)

Biometrics-based techniques

- A **biometric** is a feature measured from the human body that is distinguishing enough to be used for user authentication. (L.O'Gorman)
- Images of a person face, retina, or iris
- Fingerprints
- Footprints and gait (walking style)
- Voice patterns
- Handwriting characteristics
- Smell
- Hand geometry

Biometrics

- **Advantages**

- Biometrics can't readily be shared, copied, or stolen
- Biometrics (in normal circumstances) can 't be lost

- **Disadvantages**

- Complicated technology
- Specialized hardware
- High-cost (yet, it has been going down)

Problems with biometrics

- Certain level of
 - False positives, and
 - False negatives
- To deal with this problem one may combine biometric technique with password- or token-based techniques
- If measuring equipment is not specially protected, the equipment is vulnerable to sabotage and fraud.

Recent advances: authentication by brainwaves

- John Chuang et al.
- “I think, therefore I am: Usability and Security of Authentication Using Brainwaves”, a 2013 paper available at
- people.ischool.berkeley.edu/~chuang/pubs/usec13.pdf

Authentication using Brainwaves

- Experimental study:
 - using single channel EEG sensors embedded in wireless headsets (Neurosky MindSet ~100 USD) for authentication
 - 99% accuracy is achieved

Authentication using Brainwaves (cont.)

- Seven different (mental) tasks are used in the experiments:
 - Breathing, simulated finger movement, sport tasks, etc each taking 10 seconds
 - Brainwaves were measured and processed to distinguish the participants
 - Self-similarity and cross-similarity measures are used
- Possible project:
 - re-implement and to develop further EEG based authentication

User authentication

